TRANSPORTATION SAFEGUARDS TRAINING SITE

FY2004 Comprehensive Security & Safety Handbook - TSTS 12

Fort Chaffee Arkansas

Review, Concurrence, and Approval

Original Signed 8/10/04

Lynn Pincumbe, Facility Security Representative Date
Office of Secure Transportation

Annual Review	
Reviewed By: Lisha Hutchins	Date: 8/10/05
Reviewed By:	Date:
Reviewed By:	Date:
Reviewed By:	Date:
Reviewed By:	Date:
Reviewed By:	Date:
Reviewed By:	Date:
Reviewed By:	Date:
Reviewed By:	Date:
Reviewed By:	Date:
Reviewed By:	Date:

TABLE OF CONTENTS

SAFEGUARDS & SECURITY AWARENESS

As an employee, contractor, or subcontractor of the DOE, you have been given the opportunity to participate in some of the most sensitive programs within the U.S. government. You may also require a DOE access authorization (commonly referred to as a security clearance), which carries with it important individual responsibilities. To help you perform these responsibilities, DOE has established a Safeguards and Security Awareness Program. This program is designed to raise your individual level of awareness about your security responsibilities. You are required to participate in this program.

The objective of the Security Awareness Program is to make you aware of your security responsibilities. This knowledge is vital to your role in the overall security program. This reference handbook contains information about your security responsibilities and serves to enhance your security awareness.

Security is emphasized to protect classified information and unclassified controlled information against unauthorized disclosure, which could have an adverse impact on the nations security. The threat could be foreign or domestic to include insiders and criminal factions who will use a variety of tactics to gain access to information. Each employee's awareness of potential threats and security responsibilities is crucial to keep our nations assets secure and safe.

The Safeguards and Security Awareness Program is based on the concept that security is a state of mind as well as an individual responsibility. Various security briefings, defined below, are designed to enhance appreciation for your responsibility in protecting national security interests such as classified and sensitive unclassified information, and to foster a state of mind that will make security much more than just a routine compliance effort.

BRIEFING REQUIREMENTS:

INITIAL BRIEFING: Before assuming duties, all cleared and un-cleared employees must receive an initial safeguards and security awareness briefing. The initial briefing provides an overview of DOE safeguards and security disciplines and orients new employees to local security responsibilities and measures. Initial briefing attendance records need to be maintained with badge records or other records pertaining to access control.

COMPREHENSIVE BRIEFING: The comprehensive briefing must be given to cleared personnel after their access authorizations, but before they gain access to actual classified information or SNM. As a condition for access to classified information, SNM, or unescorted access to DOE security areas, these individuals must complete a Classified Information Nondisclosure Agreement (SF-312)*.

REFRESHER BRIEFING: DOE O 470.1, Chapter IV Safeguards and Security Awareness Program, requires all individuals who possess Department of Energy (DOE) access authorizations to receive refresher briefings to reinforce and update awareness of safeguards and security policies and their responsibilities each calendar year at approximately 12-month intervals. This briefing is designed to selectively reinforce the information provided in the comprehensive briefing as well as address current facility/organization-specific safeguards and security issues. Attendance must be documented with individual signature and badge number.

TERMINATION BRIEFING: Termination briefings are required to inform individuals of their continuing security responsibilities after their access authorizations are terminated. This briefing is conducted on whichever of the following days occurs first: the individual's last day of employment, the last day the individual possesses an access authorization, or the day it

becomes known that the individual no longer requires access to classified information or SNM. A Security Termination Statement (DOE F 5631.29) may be completed to document and acknowledge receipt of the termination briefing.

PHYSICAL SECURITY:

According to the current Federal Data Approval Record, Transportation Security Training Site is designated a property protection area.

ESCORTING: For the property protection area, escorts are required at TSTS during sensitive operations such as classified briefings, ESS, and tactical exercises. The program manager will notify Exercise Control Center prior to the commencement and end of a sensitive exercise. In addition, escorts are required in sensitive areas such as the armory and supply.

Escorts, either federal or contractor personnel must be L or Q cleared. Always keep the un-cleared person under voice control and line of sight. Announce "Un-cleared" visitors as you enter the limited area or sensitive areas to ensure that all personnel in the area have heard an "Un-cleared" person is in the area.

Challenge escorts if they are not performing their duties properly and notify the Exercise Control Center (ECC) of any problems. All visitors must report to visitor control and receive a site-specific badge for access into the property protection area. If you notice anyone inside the area without a badge ask them if they need assistance and escort them into visitor control for processing.

VOUCHING / PIGGYBACKING DOE Manuel 473.1-1: Vouching is defined as one individual visually verifying the access authorization of another person for the purpose of piggybacking into a security area. Piggybacking is defined as entering a security area with or behind a clear authorized person who has vouched for the accompanying individuals authorization for access. All persons entering security areas must have appropriate access authorization (DOE badge or Visitor Badge) a need to enter and a need to know if access to classified is involved. Vouching / Piggybacking are allowed at the vehicle gates and building 1792.

ENTERING VEHICLE GATES: It is the driver's responsibility to ensure all vehicles and personnel entering through the vehicle gates are authorized. Any unauthorized vehicle will be blocked and prevented access. ECC will be notified of unauthorized attempt to enter. ECC will notify local law enforcement as needed.

BADGES: Badges are for security ID only to enter into Department of Energy sites. They are not to be used for cashing checks or other types of identification. Report lost or stolen badges to the Badge office within 24 hours of discovery.

Do's and Don'ts: Do protect your DOE standard badge, use your badge for identification to enter into FCMTC and DOE contractor sites; Don't wear your DOE standard badge in public, or store in vehicle, or use for identification in public to cash checks or for airport security.

SECON LEVELS: For more information on SECON levels, please refer to DOE N 473.8, "Security Conditions", dated 8-7-02, and OST Federal Policy 6.02. Security Condition (SECON) levels is as follows:

- SECON-5: This condition exists when a general threat of possible terrorist activity exists but warrants only routine security measures associated with daily operations.
- SECON-4 (attack possible): This condition applies to a possible threat of terrorist activities and generally enhances security awareness responsibilities.
- SECON-3 (attack predictable): This condition is used when an increased and more predictable threat of terrorist activity exists and may increase access controls to include additional personnel and vehicle barriers.
- SECON-2 (attack pending): This condition is set when a terrorist incident occurs or intelligence information is received indicating that some form of terrorist action is imminent and requires specific protection measures to be put in place including sending non-essential personnel home.
- SECON-1(attack has occurred): This most serious condition is declared in the immediate area where a terrorist attack has occurred which may affect the site or when an attack is initiated on the site. This significantly increases protective measures and may require additional protective elements along with those in SECON-2.

INCIDENTS OF SECURITY CONCERN:

The security division conducts inquiries on incidents of security concern as outlined in DOE Notice 471.3, "Reporting Incidents of Security Concern". The Office of Inspector General (OIG) investigates allegations of fraud, waste, and abuse. Security Infractions are acts or omissions involving failure to comply with prescribed security procedures or directives for the proper protection of classified information or matter.

According to DOE N 471.3, any person with knowledge of a threat to DOE security interest must report this information to site security personnel. Examples of security concerns include but are not limited to:

- Leaving classified unattended or exposed.
- Improperly storing classified
- Failure to safeguard or account for classified resulting in compromise
- Removal of classified without proper authorization
- Improperly marking classified after classification determination has been made.
- Failure to safeguard repositories combinations
- Improper destruction of classified
- Improper transmission of classified documents
- Discussion of classified amongst uncleared personnel
- Failure to escort uncleared personnel in security areas
- Discussion of classified over unclear communication systems
- Loss of security badge
- Introducing prohibited articles into area
- Failure to safeguard computer password

If it is determined any of the above actions were intentional or negligent the employee could receive administrative sanctions or criminal prosecution.

The supervisor is responsible for administrative sanctions and disciplinary action is based on the nature and severity of the infraction. Such actions against the employee could involve:

- Verbal reprimand for first infraction during a one-year time frame. Additionally, a special security briefing may be attended.
- Written reprimand may follow a second infraction within a one-year time frame.

- Written reprimand and suspension for three days without pay is usually upon the third offense within a one-year time frame.
- Dismissal for the fourth infraction within a year is probable.

A violation is an intentional act or omission for which criminal penalties can be imposed. Examples of Security Violations include selling or stealing classified information or matter; theft of government property; and sabotage. Violations are reported to site security personnel who will assure an inquiry is initiated.

Employees with knowledge of fraud, waste, or abuse must report to the OIG Hot Line 1-800-541-1625 or NNSA OIG (505) 845-5554.

COUNTERINTELLIGENCE PROGRAM:

The role of Counterintelligence is to detect, deter, and neutralize information gathering for targeting and assessment of DOE programs, facilities, technology, or personnel by terrorists. Counterintelligence and security have joint interest in domestic terrorist activities. CI is focused on those with foreign sponsorship or direction.

Report any attempt by a person to obtain classified or otherwise sensitive information by an unusual or unauthorized request. If you believe you may be the target of actual or attempted exploitation for intelligence purposes your CI office can help. These requirements are in addition to any similar reporting requirements implemented under DOE 5670.3 COUNTERINTELLIGENCE PROGRAM.

Examples include: Market surveys sent directly to company employees rather than to the company; students or consultants using email to request sensitive information; email or telephone requests for information about sensitive programs using acronyms specific to the program.

OPERATIONS SECURITY (OPSEC):

"To secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself" Sun Tuz

OPSEC is the process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting sensitive operations and other activities. Any information that could help the adversary defeat our systems is an OPSEC concern.

As a methodology, Operations Security originated during the Vietnam War when a team was charged with learning how the enemy gained advance knowledge of combat operation In order to pinpoint vulnerabilities and recommend corrective actions, the team developed a process for analyzing operations from an adversarial viewpoint.

Today, that team's process is as applicable to administrative and R&D activities as it is to military operations. Security professionals at Los Alamos National Laboratory apply the OPSEC process to laboratory programs. The also retain the military team's wartime code name – "Purple Dragon" – as a symbol of efforts to deny the laboratory's adversaries access to sensitive information.

To prevent the inadvertent release of critical program information, follow the OPSEC five-step process:

1. Determine Critical and Sensitive Data
    - What do you want to protect?
        - Why do you want to protect it?
        - Is it governed by a regulatory requirement?
        - Can it be defined as, for example Unclassified Controlled Nuclear Information (UCNI), Export Controlled information (ECI), proprietary, privacy act etc.?
        - Do you just "feel" it should be protected?

2. Analyze the Threat
    - Who wants it?
        - Who wants the sensitive information or critical technology?
        - Is there more than one adversary?
        - What is their objective?
        - What will they do to get your sensitive information or critical technology?
        - How might they go about getting it?

3. Determine the Vulnerabilities?
    - How can they get it?
        - How is your information or critical technology vulnerable?
        - How is it protected or not protected?
        - Is it properly protected?

4. Analyze the Risk
    - What are the consequences if you lost it?
        - Is the risk great enough to do something about the threat?
        - How would the loss of sensitive data affect your program?
        - What would be the cost of losing sensitive data?

5. Develop and Implement Countermeasures
    - How can you protect it?
        - What countermeasures will block access to your information or technology? Adopt measure specific to your project and include the following:
            1. Limit Web page access.
            2. Shred sensitive hard copy.
            3. Sanitize bulleting boards.
            4. Monitor public conversations.
            5. Do not use e-mail for sensitive project communications.

Completing the OPSEC process once is not enough. You should apply to process to every project and repeat it many times during each project's duration. Skilled adversaries do not need you to reveal the entire picture of your work. They can build the picture from pieces obtained separately; for example, from a recycle bin, a Web page, or a publication. To protect the whole, you must protect the pieces.

For additional OPSEC Information: A library exists in Building 1792 with video tapes and materials on OPSEC.

PERSONNEL SECURITY PROGRAM:

PERSONNEL SECURITY PROGRAM (PSD) DOE M 472.1-1B AND DOE O 472.1B: The program was designed to determine the trustworthiness, reliability, and honesty of individuals working with information vital to our national security. The information revealed during this process is protected under the Privacy Act of 1974 and is reviewed by the requestor, investigator(s), and adjudicator(s). Any derogatory information discovered in this process could prevent an individual from receiving a clearance; however, information disclosed in a timely matter could fall under mitigating circumstances and still receive a favorable adjudication.

Your initial investigation for a "Q" could take up to one year and for an "L" six to nine months barring red flags that may expand your investigation. For new hires that are prior service depending on their previous level of clearance may request "reciprocity" thus eliminating work already performed. This request must be written in the remarks section by your requestor "Individual has prior service and reciprocity is requested". Contractors should not contact PSD directly in attempt to determine status of their clearance. Such request should be directed to the respective Contracting Officer's Representative.

In addition to your initial investigation you are required to complete a reinvestigation periodically to determine the need for continued access authorizations. The "Q" is required every five years and the "L" is required every ten years. Any changes in your status, reflected below in paragraph 2, must be reported to prevent any question of your integrity in the future.

Individuals applying for or granted DOE Access Authorizations are required to:

1. Responses to questions contained in the Questionnaire for National Security Positions must be true, complete, and correct to the best of your knowledge and belief. Knowing and willful false statements on the questionnaire may result in penalties as delineated in U.S. Code, Section 1001, Title 18.

2. Directly notify the cognizant DOE personnel security division of the following: (**NOTE: Verbal notification is required within 2 working days followed by written confirmation within the next 3 days.)**

    - All arrests, criminal charges (including charges that are dismissed), or detentions by Federal, State, or other law enforcement authorities for violations of law, other than traffic violations for which a fine of $250 or less was imposed, within or outside of the United States.
    - Personal or business-related filing for bankruptcy.
    - Garnishment of wages.
    - Legal action effected for name change.
    - Change in citizenship, and
    - Employment by, representation of, or other business-related association with a foreign or foreign-owned interest or foreign national.

HUMAN RELIABILITY PROGRAM (HRP): HRP requires initial screening and periodic evaluation of individuals who apply for or occupy certain positions critical to the national security. HRP positions have been identified by the Department of Energy as positions having direct access to significant quantities of special nuclear material or direct responsibility for transporting or protecting significant quantities, nuclear material production reactor operators, and other positions with the potential for causing unacceptable damage to the national security. Supervisors are responsible to ensure employees who occupy HRP designated positions meet high standards of reliability and currently hold a Q clearance.

Security Concerns can be actual security violations such as:

- Failing to protect classified matter or disclosing classified information to someone not authorized;
- Behavior that raises doubts about an employee's allegiance to the nation's security including personal act of sabotage, espionage, treason, sedition, or terrorism;
- Sympathetic or supportive association of organizations advocating the overthrow of the government;
- Habitual or excessive use of alcohol or illegal activity;
- Conduct that indicates a lack of honesty, reliability or trustworthiness;
- Financial irresponsibility; or Illness or mental conditions, which may cause a defect in judgment as determined by a licensed psychologist.

CYBER SECURITY:

Government owned computer systems as well as Internet and email services are for official government use with no expectation of privacy, including keystroke monitoring and review of your files and logs. Some limited personal use is allowed and you should review the site policy titled "Internet, Intranet, E-mail Policy (N0027)" which can be found at www.al.gov/cybersec/policy.htm. Internet and email services are monitored, and waste, fraud and abuse audits of computer systems are conducted regularly to ensure computer systems are being used properly, access is authorized and information is correctly labeled as to sensitivity. Policy violations, such as use of the Internet to view sexually explicit adult material or other inappropriate behavior are reported to management.

Always be aware of the classification level of the computer systems you use whether classified or unclassified. Each type has different rules that apply pertaining to user levels, connectivity to other systems, and allowable levels of data that the security plans address.

There are networked and standalone system, both classified and unclassified. Each primary network or system is "accredited" by the General Support System Security Plan that specifies the authorized conditions for use.

In addition, standalone computer systems (laptops, Personal Electronic Devices desktops, etc) or any computer system with a unique security requirement, such as a modem, requires a Micro-computer Security Plan Addendum (MSPA), which must accompany the device.

All users must complete cyber security training before receiving a user identification and password. Additionally, users must complete an annual cyber security training as directed. Users must protect passwords at all times and are prohibited from sharing passwords. Passwords must be memorized and not written down. If the system is classified the password has to be protected as if it is classified too.

Processing classified information on an unclassified system is a security incident. Users are cautioned against technical email exchanges. If you receive an email with unmarked classified or sensitive information you are required to report the incident to your site security personnel.

General User Cyber Security Information:

- Know the classification level of information you are processing. If there is any doubt regarding classification see your derivative classifier.
- Be aware of surroundings when processing information on the computer and assure only authorized individuals view the information.

- Viruses check removable mediate, e-mail attachments, and update anti-virus software regularly.
- Use strong passwords with a minimum of eight characters, which consist of upper case, lower case, special characters, and numbers. Do not write passwords down or reveal them.
- Personally owned computers or software are not authorized at the site. Non-standard software must have prior approval from the IT department and Cyber Security Team before purchasing or using non-standard software or hardware.
- Back up important data to a disk and protect disks according to content.
- Never leave laptops unattended especially when traveling.
- Do not leave an unclassified computer system logged on and unattended without locking the workstation.

TECHNICAL SURVEILLANCE COUNTERMEASURE (TSCM):

Technical Surveillance Countermeasures provide information on technology and the hazards it poses for security and how to counteract those potential threats. For instance, a conventional telephone can be turned into a microphone and all conversations in its vicinity monitored without your knowledge by a person on the other side of the world. Installation of a small device called an "infinity transmitter" into your telephone from any other telephone, prevent it from ringing and cause your telephone to become an active while still on-hook. This allows the caller to listen to sounds in your home or office without your knowledge. Also, simple modifications or the degradation of electronic components in your telephone can cause sounds in the vicinity of the telephone to be passed down the lines, even through the telephone is on-hook.

Activities can be observed by video through pinholes in your ceilings and walls. Current video technology permits viewing and recording through a hole 1/8 inch in diameter or smaller. Video signals can be transmitted over distance through walls to be monitored and recorded.

Someone can overhear conversations outside your home or office by use of a virtually invisible laser bean, focused on your window or on objects within your home, which are slightly vibrated by your voice.

A radio, pager, recorder or television may be transmitting your conversations to persons who are able to receive those signals and listen to your conversations without your knowledge. All radio, television receivers and monitors, and recording equipment require small radio frequency emitting circuits in order to work. Degradation or modification or those circuits may cause sounds in the vicinity of equipment to be transmitted into free space and made available to anyone with receiving equipment. Even though it is in violation of federal law to eavesdrop or obtain information by covert electronic means, eavesdropping has not be deterred a great degree with fines up to $10,000 and one year imprisonment; however, espionage carries stiffer penalties.

SEARCH & SEIZURE:

The degree of individual privacy considered reasonable for business premises and offices depends on the character of the work areas, the nature of the business, and the policies and procedures governing employee privacy. The general rule is this: What a person reasonably seeks to keep private is constitutionally protected. In other words, there's a reasonable expectation of privacy in private areas (those reserved for a person's exclusive use), but not in public areas.

A search occurs when the government's conduct infringes on a person's expectation of privacy. Seizure refers to any meaningful interference with a person's right to movement or possessory interest in property. A search or seizure must have a legitimate purpose, and its scope must be limited to the minimum intrusion necessary for achieving that purpose.

Government and contractor employees don't give up their Fourth Amendment rights merely because they work for the government; however, their expectations of privacy may be diminished by the operational requirements of their workplaces, as well as associated polices, practices, and procedures. A government employer does not need a warrant to search a government employee's office, desk, or file cabinet as long as there is a legitimate, non-criminal, work related purpose. Courts have held that non-government entities that contract with the government may be considered "employees of the government."

Searches for criminal evidence must be based on warrants; however, warrants are not required for non-criminal, work-related searched such as administrative searches, inspections, voluntary consent, and exigent circumstances.

- Although administrative searches do not require a warrant they must have a legitimate, non-criminal, work related purpose and must be limited to the minimum intrusion necessary to accomplish that purpose. Evidence lawfully found during such a search could be used in subsequent criminal prosecutions.
- Inspections do not require a warrant and involves the inspection of articles carried by persons entering government facilities or controlled areas. These searched do not target any specific individual and are narrowly directed to items that create a significant risk to security or safety interest.
- Voluntary consent does not require a warrant nor does the consent have to be in writing; however, the consent must be freely and competently given without threat or coercion or misrepresentation on the requestor. Employees may not be forced to choose between consenting to warrant less searches for criminal evidence and keeping their jobs.
- If there are both probable cause and imminent danger that evidence will be destroyed or disappear unless the search is conducted immediately, a warrant is not required if time would not be sufficient in receiving one.
- In addition, plain view and abandonment do not require warrants.

General principles to determine whether a search is unreasonable or violates individual rights:

- Areas for which individuals have exclusive use are protected from warrantless searches conducted to obtain criminal evidence.
- Employers do not need warrants to search for official documents or papers that are lost, missing, or needed for the business. Legitimate business reasons include protecting security and safety interest.
- Employers may search areas not reserved for an employee's exclusive use and may give consent to search for criminal activity in these areas.
- Although individual employees may consent to warrantless searches of the areas for which they have exclusive use, the supervisor may not give consent to search for criminal or non-work related evidence in areas exclusively reserved for an employee's use.

The Federal Tort Claims Act, 28 USC 1346 (B); 28 USC 2671-2680 provides a remedy against the government only for which suits may never be brought against individual employees for torts committed with the scope of employment.

POLICIES:

SURVEILLANCE DEVICES (ISSM Weekly Notice, Sept 26, 02): If a surveillance device is discovered do not disturb nor discuss in the vicinity of found device. It should be reported immediately through secure channels. Notify Technical Surveillance Countermeasure (TSCM) Officer, Kathy Sumbry-Wilkins in Safeguards and Physical Security Division. Using a "bugged" telephone or a telephone in the area of the suspected device would only alert the perpetrator and compromise any possibility of neutralizing the bugging device or apprehending the adversary.

NO COMMENT POLICY (ISSM Weekly Notice, Oct 17, 02): It is DOE policy not to comment to un-cleared persons on the accuracy, classification, or technical information in certain categories, especially the nuclear weapons design category; to do so weakens the protection provided by classification. This policy applies to articles in the public domain suspected of containing classified information even if that information is common knowledge or has been widely broadcast or published.

Statements which concern classified information appears in newspapers, magazines, books, and other publications are often based on speculation. Comments about such statements may tend to confirm or deny their accuracy and may reveal classified information.

An author or news writer may make a statement with the expectation it will be officially denied allowing him to "narrow in" on the correct information. Therefore, no comment should be made either confirming or denying classified, sensitive, or speculative information. The mere fact the "No Comment" policy applies to a specific publication is itself a classified fact. Speculating whether or not information on an open source website is classified via un-secure email constitutes a violation of the "No Comment" Policy and is in itself a compromise.

CELLULAR TELEPHONES (Policy date June 26, 2001): Cellular phones are two-way transmitting devices and pose a threat to our sensitive proprietary intellectual property. Cellular phones are not restricted by a wire such as office phones; therefore, when turned off still maintain the capability of transmitting or communicating with their cellular service provider on a continuing basis except when the battery has been removed.

Privately owned cellular telephones are prohibited from DOE security areas. Combination cellular telephones and personal digital assistants are prohibited. Government-owned cellular telephones are authorized with in the security areas but must have the battery removed.

PERSONAL DIGITAL ASSISTANTS (PDA) (Policy dated June 26, 2001): PDA's are hand held devices that are lightweight, compact, and extremely portable. They are electronic devices and range from a simple hand held organizer with very limited capabilities to a sophisticated hand-held computer with additional features such a expandable memory, scanning devices, audio recording and recognition applications, modems, snap on digital cameras and wireless connections.

These advanced technologies pose a new threat to sensitive government information and a potential for unauthorized or inadvertent disclosure of sensitive classified information especially since the PDA can be accessed or remotely activated without the user's knowledge; therefore, privately owned PDA's are prohibited from all security areas. U.S. Government purchased PDA's must have a organizational property tag securely affixed to confirm ownership and must not have the ability to record audio / video, RF capability, nor be allowed into any classified briefing.

SENSITIVE UNCLASSIFIED INFORMATION (SUI):

Sensitive Unclassified Information (SUI) is information with both national security and governmental interest. Inadvertently released information to unauthorized personnel could affect our national security. Information referred to as sensitive but unclassified information is known as Unclassified Controlled Nuclear Information (UCNI), Official Use Only (OUO), and Privacy Act Information 1974 will be discussed further. Additional information you may see is Export controlled Information (ECI), Confidential, Foreign Government Information (C/FGI-MOD), and Proprietary Information is other types of SUI.

Unclassified Controlled Nuclear Information (UCNI): Unclassified Controlled Nuclear information is located in the following orders, manuals, and guides: DOE M 471.1-1 Chg 1 *Identification and Protection of Unclassified Controlled Nuclear Information Manual* and DOE O 471.1A *Identification and Protection of Unclassified Controlled Nuclear Information.*

Unclassified Matter that contains Unclassified Controlled Nuclear Information (UCNI).

- *Front Marking.* When a Reviewing Official determines unclassified matter contains UCNI, the the front of matter is marked as follows: UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION NOT FOR PUBLIC DISSEMINATION Unauthorized dissemination subject to civil and criminal sanctions under section 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2168). Reviewing Official: _____ (Name/Organization) Date: _____ Guidance Used: _____ (List all UCNI guidance used)
- *Page Marking.* The UCNI marking must be placed on the top and bottom of the front of the matter and top and bottom of each interior page or only those interior pages with UCNI.

See DOE M 471.1-1 Chg 1 for alternative markings if matter is related to an atomic energy defense program, but does not contain any information explicitly indicating this relationship or the fact of the relationship of matter to atomic energy defense program is sensitive.

Special Format Matter. (e.g., photographs, viewgraphs, films, floppy diskettes, audio or videotapes, slides) must be marked to the extent practical as described above. UCNI must be marked so physical protection is properly provided.

Transmittal Document. A document that transmits matter marked as containing UCNI must be marked on its front as follows: Matter transmitted contains Unclassified Controlled Nuclear information. When separated from enclosures, this transmittal document does not contain UCNI.

Access tof UCNI: Access to UCNI must be provided only to those authorized for routine or special access.

- Routine Access. Routine access refers to the normal exchange of UCNI during the conduct of official business and allows for further dissemination of UCNI if the requirements below are met.
  - An Authorized Individual may grant routine access to UCNI to another person eligible for routine access to UCNI simply by giving that person UCNI. No explicit designation or security clearance is required.
  - To be granted routine access to UCNI, a person must need to know the specific UCNI in the performance of official duties. In addition to the need-to-know requirement, one of the following requirements must be met (see regulation for more information):
    - U.S. Citizen. The person is a U.S. citizen who is one of the following:
      - A Federal employee, Federal contractor or subcontractor, Federal consultant, or member of the U.S. Armed Forces.
      - A member of a State, local, or Indian tribal law enforcement or emergency response organization.

- For other than a U.S. Citizen see DOE M 471.1-1 Chg 1.

Physical Protection Requirements. The following physical protection requirements apply to matter containing UCNI.

- *Protection in Use.* An Authorized Individual must maintain physical control over any matter marked as containing UCNI to prevent unauthorized access to the information. The following are examples of information that can be UCNI: Unclassified guard force deployment; Details of communication procedure; Floor plans; Information on technology, design, or weapons related information.
- *Protection in Storage.* UCNI matter must be stored to preclude unauthorized disclosure. Store UCNI matter in locked receptacles, such as file cabinets, desks, or bookcases. When internal building security is not provided locked rooms or buildings provide adequate after-hours protection.
- *Reproduction*. Matter marked as containing UCNI may be reproduced without permission of the originator to the minimum extent necessary to carry out official duties. The reproduced matter must be marked and protected in the same manner as the original matter. Copy machine malfunctions must be cleared and all paper paths checked for UCNI material. Excess paper containing UCNI must be destroyed as described below.
- *Destruction.* UCNI matter must be destroyed by using strip cut shredders that result in particles of no more than ¼-inch wide strips. Other methods that provide sufficient destruction may be approved by the cognizant DOE security office.
- *Transmission.* Transmission must be by means that preclude unauthorized disclosure or dissemination.
  - *Outside a Facility.*
    - UCNI must be packaged in a single, opaque envelope or wrapping.
    - U.S. mail methods used: U.S. First Class, Express, Certified, or Registered Mail.
    - Any commercial carrier may be used.
    - An Authorized Individual or a person granted special access may handcarry the matter as long as access control is available.
  - *Within a Facility.*
    - A standard distribution envelope, such as Optional Form No. 65-B may be used.
    - An Authorized Individual may handcarry the matter as long as control access is provided.
  - *Over Telecommunications Circuits.* UCNI must be protected by encryption when transmitted by telecommunications services, including voice, facsimile, narrative message, communications facilities and radio communications. If UCNI is transmitted over public-switched broadcast communications paths (e.g., Internet) the information must always be protected by encryption (Entrust).

    Mission accomplishment may require the transmission of UCNI without encryption in emergency situations or when the sender or receiver requires the information for public safety or security purposes but does not have encryption capability.
    In such cases, approval to waive the encryption requirements must be obtained from (1) for Headquarters, the Director, Office of Headquarters Security Operations, Office of Security, or (2) for the field, the Operations Office Manager or Safeguards and Security Director. Such waivers are to be used only in situations where urgency precludes other more secure means of transmission. Absence of encryption capability does not justify routine unencrypted transmission of UCNI.

- *Automated Information Systems (AIS).* The AIS or AIS network must ensure that only personnel authorized for access to UCNI can access that information. For example,

networks interconnected with a public-switched broadcast network (e.g., Internet) must provide methods to ensure that UCNI is protected against unauthorized access. UCNI being transmitted over broadcast networks like the Internet, where unauthorized access is possible, must provide encryption in accordance with paragraph 2e(3) above to ensure that the information is not improperly accessed.

Violations and Infractions:

- Violation. Violation means any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of UCNI or any knowing willful, or negligent action to control information as UCNI for prohibited reasons. The Attorney General Office investigates and prosecutes s required.
- Infraction. Infraction means any knowing, willful, or negligent action contrary to the requirements of this Manual that does not comprise a violation. A DOE employee who commits an infraction is subject to an administrative penalty, as outlined in DOE O 3750.1, WORK FORCE DISCIPLINE; a DOE contractor employee who commits such an infraction is subject to such penalty as the contractor may impose.

Official Use Only (OUO): Official Use Only Information is located in the following orders, manuals, and guides: DOE O 471.3, *Identifying and Protecting Official Use Only Information,* dated 4-9-03 and DOE M 471.3-1 *Manual for Identifying and Protecting Official Use Only Information, and* DOE G 471.3-1, *Guide to Identifying Official Use Only Information*, dated 4-9-03.

To be identified as OUO, information must be unclassified and meet both of the following criteria:

- Have the potential to damage governmental interests if disseminated to persons who do not need the information to perform their jobs or other DOE-authorized activities. The possible consequences to such interests should be carefully considered in each case.
- Fall under at least one of eight Freedom of Information Act (FOIA**)** exemptions (exemptions exemption 1 covers information classified by Executive order). These exemptions describe types of information whose unauthorized dissemination could damage governmental interests.
    2) Circumvention of Statue: Internal Agency Practices such as audit criteria, parking regulations, appraisal methods; classification guides; and tests and answers.
    3) Statutory Exemption – CRADA Information, Export Controlled Information.
    4) Commercial / Proprietary: Trade secrets, financial data, business plans, and cost data.
    5) Privileged Information: Recommendations, evaluations, appraisal results, and drafts of new policies.
    6) Personal / Privacy: marital status, unlisted home number, medical files, and SSN.
    7) Law Enforcement: On-going investigative reports, reports which would impair impartial adjudication, and confidential sources.
    8) Financial Institutions: reports on financial condition of a bank.
    9) Wells: Resource maps, new drilling, and wellhead analysis.

An unclassified document that is originated within a DOE/NNSA office, produced by or for that office, or under the control of that office may contain OUO information. Any employee from an office with cognizance over such information may determine whether such a document contains OUO information. The process is as follows:

- The employee first considers if information has potential to damage if disseminated to persons who do not need the information to perform their jobs.
    - If the information is considered to have the potential for such damage, then the employee consults guidance of DOE O 471.3. If the specific information in question is

identified as OUO information in such guidance, then the employee determines the document contains OUO information.
    - If the information is considered to have the potential for such damage, but no guidance is issued about information in question, then the employee considers whether the information falls under at least one of FOIA exemptions 2 through 9 If the employee believes that the information falls under one of the FOIA I-2 DOE M 471.3-1 4-9-03 exemptions, then the employee may determine that the document contains OUO information.
- If the employee finds no basis for identifying the information as OUO in guidance issued under DOE O 471.3 and does not believe the information falls under one of the FOIA exemptions, then the employee must not mark the document as containing OUO information.

Marking Official Use Documents: The front marking includes the applicable FOIA exemption number and related category name, the name and organization of the employee making the determination, and identifies the guidance used if the determination was based on guidance. The employee making the determination ensures the following marking is placed on the front of each document containing OUO information.

- Page Marking. The employee ensures “Official Use Only” or “OUO” are placed on the bottom of each page or, on just those pages containing the OUO information.
- Marking E-mail Messages. The first line of an e-mail message containing OUO information must contain the abbreviation “OUO” before the beginning of the text. If the message itself is not OUO but an attachment contains OUO information, the message must indicate that the attachment is OUO. The attachment must have all required OUO markings.

Ensure that access to documents marked as containing OUO information or OUO information from such documents is provided only to those persons who need to know the information to perform their jobs or other DOE-authorized activities.

Protection in Use. Reasonable precautions must be taken to prevent access to documents marked as containing OUO information by persons who do not require the information to perform their jobs or other DOE-authorized activities (e.g., don’t read an OUO document in a public place, such as a cafeteria, on public transportation, etc.).

Protection in Storage. Documents marked as containing OUO information may be stored in unlocked receptacles such as file cabinets, desks, or bookcases when Government or Government-contractor internal building security is provided during nonduty hours. When such internal building security is not provided, comparable measures should be taken, such as storing the documents in a locked room or other locked receptacle (e.g., a locked file cabinet, desk, bookcase, or briefcase).

Reproduction. Documents marked as containing OUO information may be reproduced without the permission of the originator to the minimum extent necessary to carry out official activities. Copies must be marked and protected in the same manner as originals. Copy machine malfunctions must be cleared and all paper paths checked for papers containing OUO information. Excess paper containing OUO information must be destroyed as described below.

Destruction. A document marked as containing OUO information must be destroyed by using a strip-cut shredder that produces strips no more than 1/4-inch wide or by any other means that provides a similar level of destruction that has been approved by the local security office. The decision to dispose of any DOE or NNSA document, whether it contains OUO information or not, must be consistent with the policies and procedures for records disposition. Transmission.

By Mail—Outside of a Facility.

- Use a sealed, opaque envelope or wrapping and mark the envelope or wrapping with the recipient's address, a return address, and the words "TO BE OPENED BY ADDRESSEE ONLY."
- Any of the following U.S. mail methods may be used: First Class, Express, Certified, or Registered Mail.
- Any commercial carrier may be used.

By Mail—Within a Facility. Use a sealed, opaque envelope with the recipient's address and the words "TO BE OPENED BY ADDRESSEE ONLY" on the front.

By Hand—Between Facilities or Within a Facility. A document marked as containing OUO information may be hand carried between or within a facility as long as the person carrying the document can control access to the document being transported.

Over Telecommunications Circuits. Documents marked as containing OUO should be protected by encryption when transmitted over telecommunications circuits whenever possible. This may be accomplished through DOE public key systems or use of encryption algorithms that comply with all applicable Federal laws, regulations, and standards (e.g., Entrust) that address the protection of sensitive unclassified information (see Chapter 9 of DOE M 200.1-1, "Public Key Cryptography and Key Management"). However, if such encryption capabilities are not available and transmission by mail is not a feasible alternative, then regular e-mail or facsimile machines may be used to transmit the document.

By Unencrypted Facsimile. An unencrypted facsimile transmission must be preceded by a telephone call to the recipient so that he or she can control the document when it is received.

By E-mail without Encryption. If encryption is not available and some form of protection is desired, the OUO information may be included in a word processing file that is protected by a password and attached to the email message. Then the sender can call the recipient with the password so that he or she can access the file.

Transmission over Voice Circuits. OUO information transmitted over voice circuits should be protected by encryption (see DOE M 200.1-1, Chapter 9, for requirements) whenever possible. However, if such encryption capabilities are not available and transmission by other encrypted means is not a feasible alternative, then regular voice circuits may be used.

Processing on Automated Information Systems. An automated information system (AIS) or AIS network must provide methods (e.g., authentication, file access controls, passwords) to prevent access to OUO information stored on the system by persons who do not require the information to perform their jobs or other DOE-authorized activities.

CLASSIFIED MATTER PROTECTION & CONTROL:

CLASSIFICATION LEVELS AND CATEGORIES: There are three levels of classification and three categories, which signify the amount of damage to our nations security if unauthorized disclosure were to occur. The three classification levels are 1) Top Secret - exceptionally grave damage; 2) Secret - serious damage; and 3) Confidential - damage. The three categories are 1) Restricted Data (RD) - Design, utilization, and manufacture of atomic weapons or material; 2) Formerly Restricted Data (FRD) - the military utilization of atomic weapons, and 3) National Security Information (NSI) is information determined to require protection pursuant to Executive Order 12958. All classified documents are marked front, back, top and bottom to show the type

of information contained and the required level of protection. It is each individuals responsibility to report and protect such information if found un-secure until material can be properly secured.

ACCESS AUTHORIZATIONS:

The list below reflects the level of classified information badge holders are authorized to receive. The custodian of the information must ensure the individual meets the proper access level and has the need to know.

LEVEL OF CLEARANCE	Categories		
	RESTRICTED DATA	FORMERLY RESTRICED DATA	NATIONAL SECURITY INFORMATION
Q	✓	✓	✓
L		✓	✓

The Freedom of Information Act of 1996 requires that all government information be made promptly available to any person *unless exempt*. National Security Information as defined by executive order and classified information is not considered Official Use Only (OUO). Information specifically exempted from disclosure by statue includes restricted data, formerly restricted data, and Unclassified Controlled Nuclear Information (UCNI).

Access to OUO Documents containing OUO information must only be provided to those persons who require the information to perform their jobs. The responsibility for determining whether someone
has a valid need for such access rests with the person who has authorized possession, knowledge, or control of the information or document and not on the prospective recipient.

Protection of OUO: Reasonable precautions must be taken to prevent access to documents marked as containing OUO information by persons who do not require the information to perform their jobs. When internal building security is not provided, comparable measures should be taken, such as storing the documents in a locked room or other locked receptacle (e.g., a locked file cabinet, desk, bookcase, or briefcase).

Reproduction of OUO: Documents marked as containing OUO information may be reproduced without the permission of the originator to the minimum extent necessary to carry out official activities. Copies must be marked and protected in the same manner as originals. Copy machine malfunctions must be cleared and all paper paths checked for papers containing OUO information. Excess paper containing OUO information must be destroyed as described below.

Destruction of OUO: A document marked as containing OUO information must be destroyed by using a strip-cut shredder that produces strips no more than 1/4-inch wide or by any other means that provides a similar level of destruction that has been approved by the local security office.

Transmission of OUO:

- *By Mail—Outside of a Facility*. Use a sealed, opaque envelope or wrapping and mark the envelope or wrapping with the recipient's address, a return address, and the words "TO BE OPENED BY ADDRESSEE ONLY." Any of the following U.S. mail methods may be used: First Class, Express, Certified, or Registered Mail. Any commercial carrier may be used.
- *By Mail—Within a Facility.* Use a sealed, opaque envelope with the recipient's address and the words "TO BE OPENED BY ADDRESSEE ONLY" on the front.

- *By Hand*—Between Facilities or Within a Facility. A document marked as containing OUO information may be hand carried between or within a facility as long as the person carrying the document can control access to the document being transported.
- *Over Telecommunications Circuits*. Documents marked as containing OUO should be protected by encryption when transmitted over telecommunications circuits whenever possible, such as Entrust. However, if such encryption capabilities are not available and transmission by mail is not a feasible alternative, then regular e-mail or facsimile machines may be used to transmit the document.
- *By Unencrypted Facsimile*. An unencrypted facsimile transmission must be preceded by a telephone call to the recipient so that he or she can control the document when it is received.
- *By E-mail without Encryption*. If encryption is not available and some form of protection is desired, the OUO information may be included in a word processing file that is protected by a password and attached to the email message. Then the sender can call the recipient with the password so that he or she can access the file.
- *Transmission over Voice Circuits*. OUO information transmitted over voice circuits should be protected by encryption whenever possible. However, capabilities are not available and transmission by other encrypted means is not a feasible alternative, then regular voice circuits may be used.
- *Processing on Automated Information Systems.* An automated information system (AIS) or AIS network must provide methods (e.g., authentication, file access controls, passwords) to prevent access to OUO information stored on the system by persons who do not require the information to perform their jobs or other DOE-authorized activities.

Privacy Act Information: Information under the Privacy Act of 1974 requires written consent before release includes marital status, number and sex of dependents, gross salary, educational degrees and major areas of study, school and year of graduation, home address and phone, age and date of birth. Information, which does not require consent, includes information for use within DOE or employees with a need to know, position title, pay date and information releasable under the FOIA. All information must be protected from unauthorized access.

Safeguarding: If you store Sensitive Unclassified Information outside the limited area it must be in a locked desk, cabinet, file, room, or building. Documents inside of a limited area must be kept in a desk, overhead bin, or a file cabinet – out of sight out of mind. The individual in charge of the document is responsible for the release of information and must ensure the receiver has a need to know. At all cost, information must be protected from unauthorized disclosure.

Accountable Documents: All information secret and above is accountable by recording each record onto an inventory form which is maintained in the repository.

Reduction of Classified Holdings: Reviewed annually, keeping in mind records management requirements and moratoriums. Due June 30, annually.

Classified Document Custodians: Custodians are listed on the SF 700 and serve as nucleus for incoming/outgoing classified. The Exercise Control Center (ECC) is the repository center for TSTS. Custodians are responsible to verify the need to know and proper clearance level prior to release of information.

Need To Know: What is it and who makes it? It is a determination that in the performance of Official Duties, the information is required. The individual possessing the information makes the determination. Misnomer – is that it only applies to classified information; it applies to all data.

STORAGE AND PROTECTION OF CLASSIFIED INFORMATION:

SF-700, Security Container Information: Required for all containers or vault-type rooms that safeguard classified. Organizations maintain a list of all who have combination. Combination changes are required when:

- A person with the combination is no longer in the organization
- Changes to access authorizations for personnel with the combination
- Container left open and unattended
- Combination is compromised
- Upon receipt/turn-in of the container

Part 1 of the SF 700 must be completed and affixed to the security container on the inside of the locking drawer. On rooms or vaults, Part 1 must be affixed to the inside of the door containing the combination lock. Everyone knowing the combination must be listed on the SF 700. This form is used for emergency notification in the event the container is found open.

Part 2 with the recorded combination will be stored in a repository, GSA approved, with the same graded protection as required by the repository materials are stored in. If any information in the safe is accountable then part 2 is accountable and must be entered into the inventory. The SF 700 will be marked with the letter "A" in the upper right hand corner to indicate accountable. A unique tracking number is not required on the SF 700.

SF 701 Activity Security Checklist: Checklist is used for end of the day security checks. You may add to the list any additional item you would like checked for security or safety purposed such as coffee pots and windows. The forms must be maintained for ninety days. A new form will be used for each month.

SF 702 Storage Container Check Sheets: All OST activities must document when the containers are opened and closed on the SF 702. When a container is not opened due to inactivity, such as a holiday or weekend, no entry is required. On work days when the containers are not accessed an entry for that date indicating the container was checked must be made with a line where the check will be annotated and Did Not Open (DNO) across the line or write not opened to precluded information being added after the fact. Upon closure, someone other than the person who closed the safe should verify safe secure. The forms must be maintained for ninety days. A new form will be used for each month. The SF 701 and SF 702 will reflect active and non-active days and match accordingly.

AL Form 5632.1C Repository Maintenance Forms: Forms will be maintained and affixed to all security containers, safes, vaults, and vault type rooms and will be retained for the life of the container. The forms will document equipment malfunctions, repairs, and standard maintenance to assist in determining replacement requirements and help maintenance personnel diagnose problems.

Cover Sheets: Cover sheets will be used to cover all classified documents when they are removed form a secure storage. Only the Secret (SF 704) and Confidential (SF 705) will be used at TSTS.

Reproduction of Classified: Reproduction must be limited to the minimum number of copies consistent with operational requirements and with caveats on the documents. Only one approved machines inside 1792. Signs denote approval or disapproval. Sanitize machine after use by running five blank sheets of paper through the machine. The blank sheets must be shredded and treated as classified waste. Assure the shredder is sanitized.

DOE F5635.3 Classified Receipt Document: Required for all accountable matter leaving the Site (regardless of mode). Receipts must identify classified contents, names and classified addresses of both the sending and receiving facilities. Receipts must not contain classified information. For Confidential matter a listing of what is removed is required for comparison upon return.

Rest Over Night (RON): Funds, firearms, medical items, controlled substances, precious metals, or other items susceptible to theft shall not be stored in the same secure storage repository used to store classified matter.

HAND CARRY OF CLASSIFIED: Division Director approves (list or memo) in writing and those who hand carry must be knowledgeable of responsibilities.

Outside DOE Facilities During Normal Duty Hours: All classified matter to be hand-carried outside an approved facility must be double wrapped (outside and inside wrap). The inner wrap must have appropriate level and category markings on front / back and top / bottom. A classified mailing address must be listed for sender and receiver and can be the same address. The person hand-carrying the material will remain in direct possession of the package at all times until the destination has been reached. An outer container, which prevents viewing of the inner contents and is tamper resistant, such as a briefcase or pelican case is acceptable as an outer wrap.

Travel Off Site and Outside of Normal Duty Hours: Removing classified matter from approved facilities to private residence or other unapproved places (hotel, motel, bars) is prohibited. Arrival times outside of normal duty hours must be pre-arranged with receiving facility through host security office.

Commercial Air Travel: All passengers and carry on items must be screened prior to boarding. If classified material is hand-carried commercially the approved employee must not provide access to classified by unapproved individuals to prevent unauthorized disclosure.

Guidance is provided in the Federal Aviation Administration circular 108-3.

The package should be double wrapped and not contain any metal. Reporting to the airline or airport security is not required, however, processing early to avoid potential problems is advised. Process through screening as normal allowing the documents packages to be x-rayed if classified information cannot be revealed with this process. If screeners ask you to open the package, provide the screener with the original copy of your authorization letter and ask for the supervisor. At this time, the traveler must inform the carrier representative classified matter is being carried and should present official U.S. Government identification and travel documentation.

If normal processing is not possible due to contents of the package revealing classified information, the traveler will report to the air carrier at the ticket counter and the traveler may be asked to report to screening for routine processing where the package will be x-rayed. If the contents of the material would reveal classified information through x-ray, the traveler must have a Letter of Authorization to preclude x-ray screening. If the official inquires about the contents, the traveler will display the Travel Authorization Letter and explain the package is classified.

The letter will contain the following information about the traveler: name, company, type of identification, physical description of traveler, physical description of package, departure points, destination and any know transfer points;

The letter will have effective dates of expiration not to exceed seven days of issue; title, signature, and telephone number of the official issuing the letter with matching signature on the face the container exempt from screening; name and telephone number of the responsible security office to verify the classified nature of the matter. The letter must be original and on agency letterhead.

If the screener is not satisfied with provided information the traveler will not board the commercial aircraft and will immediately notify your supervisor as well as the intended receiver.

CMPC TRAINING – The DOE M 471.2-1C mandates the training and the site CMPC Procedures Manual further qualifies that all individuals acting as custodians shall receive initial training and recurring training every two years.

EMERGENCY MANAGEMENT AND RESPONSE ACTIONS:

The U.S. Department of Energy (DOE), TSTS is committed to protecting the health and safety of all its employees, contractors, and visitors. Protective actions involve either sheltering in place or evacuation. During hours of operations, the Emergency Manager will advise of protective actions through Exercise Control Center; however, after hours the CQs are to alert personnel in the event sheltering or evacuation is required. After the event, Areas of assembly have been determined as Primary and Secondary. The Primary is located between 2nd and 3rd Avenue, east of the barracks, by the tennis court. The Secondary is located North of the Physical Fitness Building. The team leads, supervisors, or program managers will need to account for each individual.

DOE has assigned designated Building Emergency Team (BET) members. The BET's are trained in emergency response procedures. Follow their instructions during an emergency. In all Emergencies 911 is the primary number to contact. After hours of operation, someone will need to meet emergency vehicles to assure immediate access to the victim is available, i.e. barrack entranceways.

Fire Prevention/Evacuation: The majority of offices are equipped with automatic sprinkler systems and there are portable fire extinguishers located near the building exits. Your buildings contain an evacuation route map. Make sure you know where the exits are located and how you will proceed to them in the event of an alarm. Should an alarm sound, leave your room and close the room door, then move out an exit as quickly as possible. DO NOT TAKE THE TIME TO SECURE PERSONAL ITEMS.

Discovery of a Fire: If you discover a fire, immediately call 911. Make sure all personnel within the area are notified of the fire and initiate evacuation of the area. Once all personnel are clear of the danger area use a telephone from a safe location to call 709-5300 Ext 5302 (day), 461-5181 (after hours) or send a messenger to notify the ECC. Do not attempt to fight a small fire unless you have been trained in the use of a fire extinguisher. NEVER PLACE YOURSELF IN HARMS WAY.

Off-Site Hazardous Materials Release: Follow the same procedures for evacuation as for a fire and go to the primary assembly area for your building. If there is a cloud of aerosolized or aromatic materials, go to an alternate assembly area that is UPWIND of the primary.

High Winds/Tornado Alert:: All OST facilities at Fort Chaffee are of similar construction and no building will afford a higher degree of protection or shelter than another. Therefore, upon receiving a high wind or tornado alert, personnel should remain in the building preferably the interior hallway on the lowest floor. Keep all winds closed and avoid all window that face south or west. Use a mattress or chair to protect yourself from debris. If no such shelter exists, seek shelter in a ditch or a ravine by staying low as deaths have occurred from flying debris. An automobile is unsafe during a tornado. Report to the assembly area when it is safe to do so.

Bomb Threat: Follow the same procedures for evacuation as for fire and evacuate to the primary assembly area. If you are the person who receives a bomb threat call, use the prompt card near the telephone to record:

- The date and time of the call
- The sex, estimated age and race of the caller
- Exact words/speech pattern of the caller
- Location of the bomb; Time of detonation
- What the bomb looks like
- Type of explosive

- Reason for placing the bomb
- Name and affiliation of any organization
- Any other information the caller will provide
- Notify the 911 and ECC at 5302 as quickly as possible

Report any suspicious objects to 911. Note: Do not activate any electrical device within 300' to include radios, cellular telephones, and lights.

Flooding: All OST facilities at Fort Chaffee are at approximately the same height above sea level, 400 feet, and are located on fairly level terrain. All facilities are subject to the same flooding threat. If flooding is imminent and there is little warning, all personnel should proceed to nearby buildings or areas located at higher elevations. If caught outside, personnel should make their way to the nearest higher elevation, even if the higher elevation poses a greater threat of lightning strike. Avoid dry creeks and riverbeds. When all personnel have reached a higher elevation than the anticipated flood crest, they may then proceed to areas that are safe from both flooding and lightning.

Earthquakes: Arkansas lies on the Central United States Seismic Zone which as the potential for a devastating earthquake. The potential for sever damage exists. For this reason, the following safety tips are recommended:

- If you are outdoors, stay outdoors. If indoors, stay indoors.
- If indoors, take cover under sturdy furniture, doorways, or along inside walls away from windows.
- If outdoors, move away from buildings and utility wires. The greatest danger is from falling debris. Get to open areas.
- If in a moving car, stop quickly and safely, away from power lines, bridges and over passes. Stay inside the car.

Lightning: The ECC has a lightning alert system that gives 12-mile, 8-mile, and 5-mile lightning strike warnings. When lightning strikes within 5 miles of an outdoor training activity, training will be stopped and all persons directed into motor vehicles. When lightning strikes within 5 miles of the compound, all outside activities within in the compound are stopped and personnel will return into buildings. The ECC representative or a Cadre member will determine when it is safe to resume outdoor activities.
The general precautions related to lightning include:

- Stay inside buildings or vehicles.
- Stay away from electrical outlets, windows, open doors, metal objects, flammable materials, hilltops, open spaces, and wire fences.
- Do not use the telephone, cellular telephone, or computer.
- If caught outside, stay away from tall structures and trees, assume a crouched position in the open.
- If the hair on the back of your neck stands up or tingles, immediately drop to the ground and crouch.

EMPLOYEE RESPONSIBILITIES AND RIGHTS UNDER THE OCCUPATIONAL SAFETY AND HEALTH ACT (OSHA):

Safety Requirements: Each employee shall comply with applicable OSHA standards, rules, regulation, Executive Order 12196, and the Federal Employee Occupational Safety and Health Program as defined in DOE Order 3790.1B and DOE Order 440.1.

Rights of Employees: Employees are granted the following rights in the workplace to assure health and safety: Right to a safe and healthful workplace; Abatement of unsafe or unhealthy conditions. Whenever prompt abatement cannot be achieved, an abatement and summary of interim steps to protect employees. Employees exposed to the conditions shall be informed of the provision of the plan; Immunity from disciplinary action or discrimination; anonymity to those making the report.

Responsibilities of Employees: Employees shall use safety equipment, prescribed personnel protective equipment, and other devices and procedures provided or directed for their protection; Notify immediate supervisor of any unsafe or unhealthy condition; Support and cooperate with safety and health personnel when they conduct inspections or investigations; Participate in the safety and health program. Employees may be authorized official time with supervisory concurrence to participate in certain safety and health program activities.

Reporting Job Related Injury / Illness: Notify immediate supervisor of any job related injury, illness, or accident and if necessary see treatment promptly. No employee is subject to restraints, interference, coercion, discrimination, or reprisal for filing a report of unsafe or unhealthy working conditions.

Construction Sites: Our site is growing continuously with the assistance of commercial construction. There are risks involved with such construction and for your own protection please refrain form entering an area zoned for construction. Your restraint from crossing over or through barriers is paramount to your safety.

Hazard Communication: The Material Safety Data Sheets (MSDS) are required by law to be provided by the manufacturer for all chemical agents. Every chemical agent stored at this site will have a copy of the MSDS provided to ES&H. The MSDS contains critical information about the chemical's health hazard, first air/decontamination measures, and proper storage and handling. Employees are reminded to not remove labels from products or place products in un-labeled containers for use.

SECURITY & SAFETY BRIEFING

We hope these briefings are informative and assist you in fulfilling your daily security responsibilities. This year we are trying a new approach in scheduling and how we are tailoring the presentations to the organization(s). We are also supplementing our presentations with handouts. We would like feedback on the information presented and this approach.

Please be as candid as you like with your comments so we can improve.

Comments on Presentations: _____

Comments on Content of Information: _____

Comments on This Approach: _____

Comments on Handouts: _____

Comments on Scheduling: _____

General Comments: _____

_____ _____

(Name is Optional) (Date)

Thank you for your comments. Please return to: Lisha Hutchins, Program Analyst

Security & Safety Briefing Acknowledgement

I have read and understand the material provided to me to fulfill the Security and Safety Briefing requirements. I have been informed that if I have any questions or concerns I can contact the Security Administrator at TSTS (479) 709-5300 ext. 5319.

PRINTED NAME AND SIGNATURE DATE:

BADGE NUMBER